



MP1800-20系列3G路由器用户手册

MAIPU



本手册著作权属迈普通信技术股份有限公司所有，未经著作权人书面许可，任何单位或个人不得以任何方式摘录、复制或翻译。
侵权必究。

策 划： 研究院 资料服务处

* * *

迈普通信技术股份有限公司

地址：成都市高新区九兴大道 16 号

技术支持热线：400-886-8669

传真：（028）85148483

E-mail: support@mail.maipu.com

网址: <http://www.maipu.com>

邮编：610041

* * *

版次：2011 年 5 月第 1.0 版

编号：MP/DC-RD-CPSJ-110-R2011-0020



目 录

第1章	约定说明	4
1.1	目的	4
1.2	适用范围	4
1.3	本书约定	4
1.4	专用术语	5
第2章	产品介绍	10
2.1	技术规格	10
2.2	功能特点	11
2.3	产品型号	11
2.4	产品形态	12
第3章	联机登陆	14
3.1	环境要求	14
3.2	使用准备	14
3.3	配置计算机	15
3.4	登录系统	19
第4章	配置操作	20
4.1	系统	20
4.1.1	系统时间	20
4.1.2	远程日志	22
4.1.3	管理控制	23
4.1.4	配置管理	23
4.1.5	系统升级	24
4.1.6	SNMP	25
4.1.7	修改密码	25



4.1.8	重启系统	26
4.1.9	退出登录	26
4.2	网络	26
4.2.1	拨号接口	27
4.2.2	LAN接口	31
4.2.3	转发模式	31
4.2.4	动态域名	32
4.2.5	静态路由	33
4.2.6	动态路由	33
4.3	服务	35
4.3.1	DHCP设置	35
4.3.2	热备份	38
4.4	状态防火墙	39
4.4.1	基本设置	40
4.4.2	访问控制	40
4.4.3	端口映射	42
4.4.4	MAC-IP绑定	42
4.5	QOS	43
4.5.1	带宽管理	43
4.6	VPN配置	44
4.6.1	IPSec	44
4.6.2	L2TP	51
4.6.3	GRE	53
4.6.4	证书上传管理	55
4.7	状态	58



4.7.1	系统日志	58
4.7.2	系统信息	59
4.7.3	IPSec隧道状态	60
4.7.4	拨号接口状态	60
4.7.5	LAN状态	62
4.7.6	路由信息	63
4.7.7	DHCP信息	63
4.7.8	连接信息	63

第5章	常见问题解答	65
-----	--------------	----



第1章 约定说明

本章向您介绍了阅读本手册和使用迈普®MP1800-20系列3G路由器的一些约定及说明。

1. 目的
2. 适用范围
3. 本书约定
4. 专用术语

1.1 目的

本说明书用于指导迈普® MP1800-20系列3G路由器的安装调试、使用及维护。

1.2 适用范围

1. 本说明书适用的对象包括：
 - n 具有一定计算机通讯、网络、电子技术等知识的人员
 - n 具有网络设备管理经验的人员
 - n 其他需要使用迈普® MP1800-20系列3G路由器相关管理人员
2. 适用的产品型号：SJW12-C-AC、SJW12-W-AC、RM1800-20C、RM1800-20W

1.3 本书约定

1. 符号、图标约定：

为了方便您快速阅读本说明书，下表是我们和您的一些阅读约定：



表1-1: 约定说明表

约定项	释义说明	备注
MP1800-20	指迈普® MP1800-20系列3G路由器产品	出现在第二章之后的过程中
&	提示: 提醒使用者或者相关阅读者需要特别记住的一些重要信息或者参数说明	出现在本手册使用操作过程中
%	注意: 提示用户某些非法操作或者配置将会出现	出现在本手册第一章之外的说明过程中
à	表示在配置管理界面进行的“下一步”操作提示	出现在配置管理操作章节

2. 配置操作约定

为了使本手册内容简洁不重复,我们对MP1800-20 路由器Web管理界面上的“保存”、“刷新”、“取消”、“复位”、“提交”按钮的操作将不做每个配置过程的一一说明,在此统一约定为:

- n **【保存】:** 任何一个配置操作动作在配置完成后,都需要点击该按钮提交至系统生效。
- n **【刷新】:** 当某个配置页面信息因为配置保存后未发生改变,通过该按钮可以快速刷新页面显示信息。
- n **【取消】:** 撤销已填写好的配置参数,点击该按钮。
- n **【复位】:** 清空页面所有输入框内容。
- n **【提交】:** 将页面配置数据上传至服务器。

1.4 专用术语

本手册所涉及的技术专用术语说明如下:

APN	接入点名称 Access Point Name
APP	应用业务 Application
ATM	异步转移模式 Asynchronous Transfer Mode
ATM	自动柜员机 Auto Table Machine
AuC	鉴权中心 Authentication Centre



BG	边际网关 Border Gateway
BGP	边际网关协议 Border Gateway Protocol
BSC	基站控制器 Base Station Controller
BSCC	基站控制连接 Base Station Control Connection
BSS	基站系统 Base Station System
BSSGP	基站系统GPRS协议 BSS GPRS Protocol
BTS	基站收发系统Base Transceiver System
CDMA	码分多址 Code Division Multiple Access
CDR	呼叫详细记录 Call Detail Record
CGF	计费网关功能 Charging Gateway Function
CSD	电路交换数据 Circuit Switch Data
DDN	数字数据网 Digital Data Network
DDP	DTU DSC通信协议 DTU DSC Protocol
DHCP	动态主机配置协议 Dynamic Host Configuration Protocol
DNS	域名系统 Domain Name System
DSC	数据业务中心 Data Service Center
DTU	数据终端单元 Data Terminal Unit
EGP	外部网关协议 External/Exterior Gateway Protocol
EIGRP	外部Internet组路由协议 External/Exterior Internet Group Routing Protocol
EMC	电磁兼容 Electro Magnetic Compatibility
ESP	静电防护 Electro Static Precautions
ETSI	欧洲电信标准协会 European Telecommunications Standards Institute
GGSN	GPRS支持节点网关 Gateway GPRS Support Node
GMSC	移动交换中心网关 Gateway MSC
GPRS	通用分组无线业务 General Packet Radio Service
GSM	全球移动通信系统 Global System for Mobile Communications
GSN	GPRS支持节点 GPRS Support Node
GTP	GPRS隧道协议 GPRS Tunneling Protocol
GTP-id	GTP标识 GTP Identity
HLR	注册地信息注册器 Home Location Register
HSCSD	高速电路交换数据 High Speed Circuit Switch Data



ICMP	网际控制信息协议 Internet Control Message Protocol
IGMP	互联网组管理协议 Internet Group Management Protocol
IGRP	互联网网关路由协议 Internet Gateway Routing Protocol
IN	智能网 Intelligent Network
IP	互联网协议 Internet Protocol
IPv4	IP协议第4版 IP version 4
IPv6	IP协议第6版 IP version 6
IPSEC	IP安全协议 IP Secure Protocol
ISDN	综合数字业务网络 Integrated Services Digital Network
ISP	互联网业务提供商 Internet Service Provider
L2TP	第二层隧道协议 Layer 2 Tunneling Protocol
LA	位置区域 Location Area
LLC	逻辑链路控制 Logical Link Control
MAP	移动应用部分 Mobile Application Part
MDNS	移动域名系统 Mobile Domain Name System
MDTU	移动数据终端单元 Mobile Data Terminal Unit
MIB	管理信息库 Management Information Base
MS	移动台 Mobile Station
MSC	移动交换中心 Mobile Switching Center
MT	移动终端 Mobile Terminal
MTBF	平均故障时间 Mean Time Between Failure
MTTR	平均维护时间 Mean Time To Recovery
MTU	最大传输单元 Maximum Transmission Unit
N/A	不可用 Not Applicable
NAS	网络接入服务器 Network Access Server
NAT	网络地址转换 Network Address Translation
NTP	网络时间协议 Network Time Protocol
O&M	运行和维护 Operations & Maintenance
PAP	密码授权协议 Password Authentication Protocol
PCF	分组控制功能 Packet Control Function
PDP	分组数据协议 Packet Data Protocol



PDN	分组数据网络 Packet Data Network
PDSN	分组数据服务器 Packet Data Service Node
PLMN	公众陆地移动网络 Public Land Mobile Network
POS	销售终端 Point of Sales
PTM-G	点对多点群呼 Point-to-Multipoint Group Call
PTM-M	点对多点多播 Point-to-Multipoint Multicast
QoS	服务质量 Quality of Service
RA	路由范围 Routing Area
RADIUS	远程授权拨入用户服务 Remote Authentication Dial In User Service
RIP	路由信息协议 Routing Information Protocol
RSC	注册业务中心 Register Service Center
RTOS	实时操作系统 Real Time Operating System
RTP	实时传输协议 Real-time Transport Protocol
RTU	远方终端单元 Remote Terminal Unit
RSVP	资源预留协议 Resource Reservation Protocol
SCADA	监控与数据采集系统 Supervisory Control and Data Acquisition
SGSN	GPRS服务支持节点 Serving GPRS Support Node
SIM	用户标识模块 Subscriber Identity Module
SMS	短消息业务 Short Message Service
SMSC	短消息服务中心 Short Message Service Center
SNMP	简单网络管理协议 Simple Network Management Protocol
STK	SIM卡工具包 SIM Tool Kits
TCP	传输控制协议 Transmission Control Protocol
TDMA	时分多址 Time Division Multiple Access
TMN	电信管理网络 Telecommunication Managed Network
UDP	用户自带寻址信息协议 User Datagram Protocol
UIM	用户标识模块 User Identity Module
UMTS	通用移动通信系统 Universal Mobile Telecommunication System
USSD	非结构化补充业务数据 Unstructured Supplementary Service Data
UTK	UIM卡工具包 UIM Tool Kits
VLR	访问地注册器 Visitor Location Register



VPN	虚拟专用网 Virtual Private Network
VRRP	虚拟路由冗余协议 Virtual Router Redundancy Protocol
WAN	广域网 Wide Area Network
WAP	无线应用协议 Wireless Application Protocol
WDDN	无线DDN Wireless Digital Data Network



第2章 产品介绍

本章主要向您介绍MP1800-20路由器的规格、功能以及产品型号等特点，让您对MP1800-20路由器有一个初步的印象，这对您以后充分使用本产品有很好的帮助作用。

1. 技术规格
 2. 功能特点
 3. 产品型号
 4. 产品形态
-

2.1 技术规格

1. 3G数据

§ 支持两种制式的3G模块，分别支持WCDMA和CDMA2000两种网络制式

2. 接口

§ 天线接口：50Ω/SMA 阴头

§ SIM/UIM卡：3V

§ 串行数据接口(RJ45)：RS-232(DCE)

§ 串行数据接口速率：9600 bits/s

§ 以太网接口：10/100BaseT/RJ45 自适应

3. 供电

§ 电压：+5VDC

4. 功耗

§ 空闲：800mA@+5VDC

§ 最大：2A@+5VDC

5. 其他参数

§ 尺寸：小于100mm×130mm×30mm (不包括天线和安装件)

§ 重量：小于500g

§ 工作环境温度：-5~+55℃

§ 储存温度：-20~+70℃



- § 工作环境相对湿度
 - n 长期：40%~65%
 - n 短期：10%~90%
- § 存储相对湿度：0~95%

2.2 功能特点

1. 基本特点

- § 使用方便、灵活、可靠
- § 支持CDMA 2000、WCDMA
- § 数据终端永远在线
- § NTP网络校时
- § 远程日志
- § 远程SSH、Telnet、HTTP管理
- § 本地Firmware升级/配置备份
- § SNMP管理
- § 支持DDNS
- § 内置DHCP、VRRP服务
- § 防火墙与虚拟地址转换(NAT)
- § 支持封包过滤
- § 支持移动网络流量统计
- § 支持VPDN、APN专网接入

2. 增强功能

- § 支持IPSEC、L2TP、GRE
- § 支持国密算法SM1
- § 支持离线数字证书
- § 支持按需拨号和永久在线
- § 支持静态路由、动态路由RIPv2

2.3 产品型号

MP1800-20路由器是采用通用基础平台、个性化应用的设计指导思想开发的产品，以适应不同的行业应用需求和运营商的网络环境。目前，MP1800-20路由器使用MP1800-20平台，有多种不同的型号选择，为了区分具体的产品型号，特说明如下：

MP1800-20路由器型号：RM1800-20x、SJW12-x-AC



表2-1:产品型号列表

RM1800-20	x
迈普MP1800-20 路由器通用平台	W-WCDMA C-CDMA2000
SJW12	x
带SM1国密算法的路由器通用平台	W-WCDMA C-CDMA2000

2.4 产品形态

1. 前面板

RM1800-20x:



SJW12-x-AC:



RESET: 复位按钮，带电情况下按2~3秒则系统复位；长按6~10秒设备恢复出厂设置。
CONSOLE: 串口控制台，波特率为9600，8位数据位，无校验，1位停止位。
LAN: RJ45以太网接口。

根据指示灯的状态可以判断路由器当前的状态:

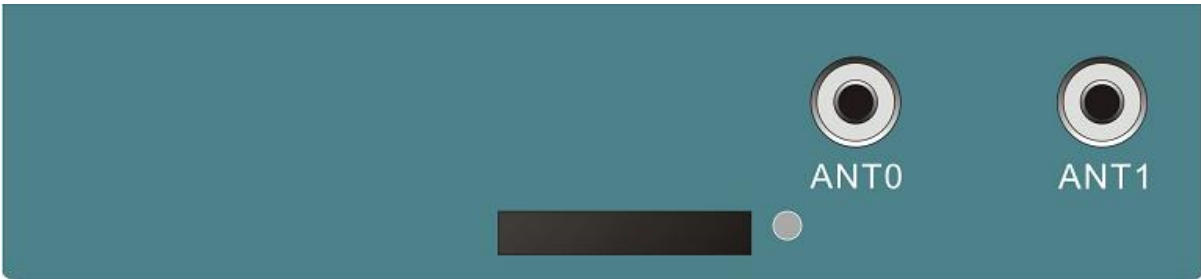
指示灯	状态	描述
系统指示灯（SYS）	绿色常亮	设备正常供电，并且处于启动状态



	绿色闪烁	设备正常运行
以太网指示灯（LAN）	绿灯常亮	以太网连接已建立
	绿灯闪烁	以太网正在传输数据
3G指示灯（3G）	绿色闪烁	3G网络有数据传输

2. 后面板

RM1800-20x:



SJW12-x



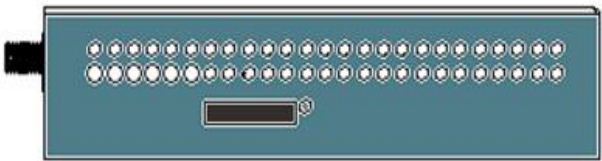
注:

- 1、ANT0为主天线
- 2、外置电源适配器为DC 5V/2A
- 3、SIM卡槽的位置如下:

RM1800-20x:



SJW12-x-AC:





第3章 联机登陆

本章主要向您介绍MP1800-20路由器的使用要求、安装接线及配置登陆过程，可以帮助您顺利登陆本产品的管理系统。

1. 环境要求
2. 使用准备
3. 配置计算机
4. 登陆系统

3.1 环境要求

MP1800-20路由器对使用环境的要求：

- § 工作环境温度：-5~+55℃
- § 储存温度：-20~+70℃
- § 工作环境相对湿度
 - n 长期：40%~65%
 - n 短期：10%~90%
- § 存储相对湿度：0~95%

3.2 使用准备

配置使用MP1800-20路由器时，通常需要按如下要求准备：

- § 计算机一台：
 1. 配有以太网卡和TCP/IP协议的计算机
 2. IE 8.0浏览器（其他浏览器也能保证功能可正常使用）
 3. 建议采用1024x768分辨率显示
- § UIM(/SIM)卡一张



% 注意:

设备正确的启动顺序为：先插SIM卡 à 插天线 à 上电。如果启动顺序不当，可能导致设备的功能无法正常使用！

3.3 配置计算机

下面以局域网连接方式，并选用Windows XP系统为例介绍计算机网络连接配置步骤。

1. 方法一

首先在局域网选择一台计算机作为配置用机，进入“控制面板” à “网络连接”，如下图，此页面上选择对应网卡的“本地连接”。



图3-1. 配置电脑本地连接

进入（双击或右键击）“本地连接” à “属性(R)” 进入下图：



图3-2. 配置电脑本地连接属性

选择“Internet 协议 (TCP/IP)”，点击“属性(R)”，进入下图：

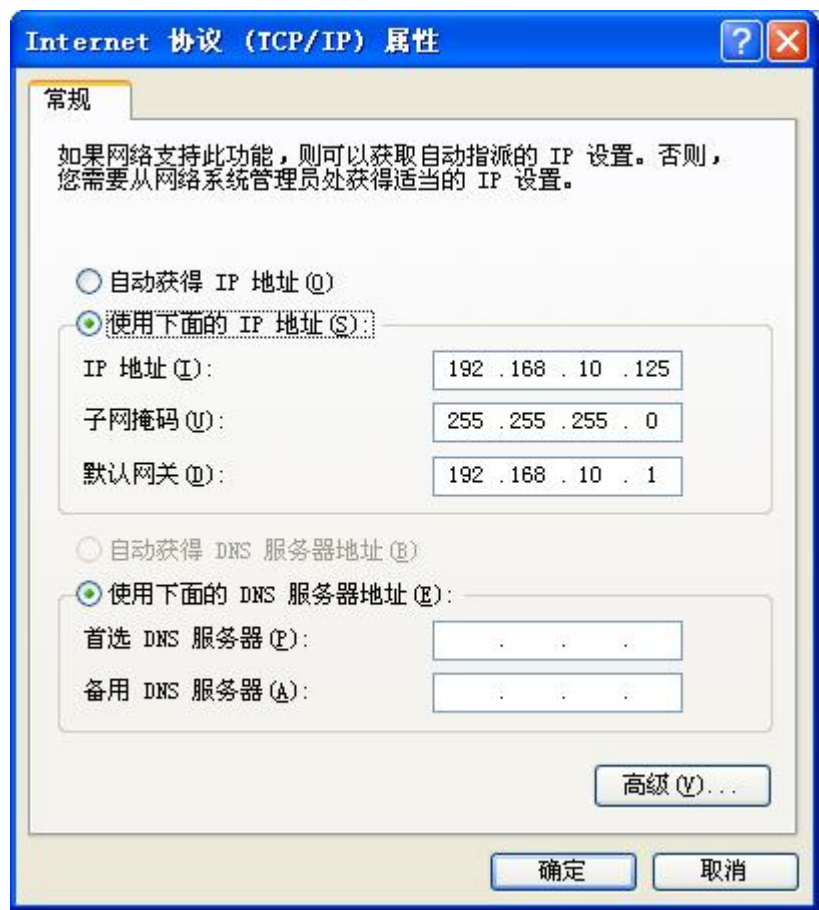


图3-3. TCP/IP属性配置

配置如下：
IP地址：192.168.10.* （*表示2-254任意整数）
子网掩码：255.255.255.0
默认网关：192.168.10.1

配置完成后，点击“确定”即可。

- % 注意：**
- 1. 此方法会暂时中断配置电脑与局域网的通信。
 - 2. MP1800-20路由器RJ45接口出厂设置：
 - § IP地址：192.168.10.1
 - § 子网掩码：255.255.255.0



2. 方法二

在原有网络配置环境下，当您不希望中断本地PC机继续与局域网通信，又能对MP1800-20路由器进行配置时，您可以考虑通过添加路由（IP）方式来实现。

点击上图3-3中的“高级(V)”按钮，进入下图：



图3-4. TCP/IP属性高级配置界面

点击图3-4中的“IP地址(R)”项中的“添加(A)”按钮，填写您要添加的IP地址，如下图，



图3-5. TCP/IP地址添加界面

配置完成点击“添加”即可，此时添加了一条到达MP1800-20路由器的路由了。

& 小技巧：

如果您仅是配置MP1800-20路由器，我们建议您选择“方法二”，这样会更省时间！

3.4 登录系统

打开配置电脑IE浏览器，在地址栏内输入：<http://192.168.10.1/>

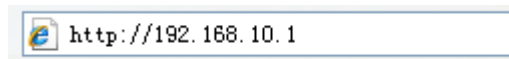


图3-6. web登录

按回车键进入用户登录界面如下图：



图3-7. 用户登录验证

用户初次登录系统时，须使用缺省密码：

§ 密码：admin

正确输入密码后，就可以登录MP1800-20路由器 WEB配置界面了。



第4章 配置操作

本章主要向您介绍如何通过Web管理界面配置使用MP1800-20路由器，详细向您说明了本产品的各个功能特点、配置参数以及配置注意事项和问题。

1. 系统
2. 网络
3. 服务
4. 状态防火墙
5. QoS
6. VPN配置
7. 状态

4.1 系统

MP1800-20路由器系统工具为方便您管理系统提供以下功能：

- n 系统时间
- n 远程日志
- n 管理控制
- n 配置管理
- n 系统升级
- n SNMP
- n 修改密码
- n 系统重启
- n 退出登录

4.1.1 系统时间

MP1800-20提供两种时钟同步方式：手动设置和网络时间。

p 手动设置

进入“系统”à“系统时间”，看到如下图手动设置时间配置界面：



系统时间

当前时间	2011年04月01日,12:30:01	
系统时间设置	手动设置 ▼	
日期设置	2011-04-01	*
时间设置	12:30:00	*

✕ 取消

✔ 保存

图4-1. 手动设置时间界面

- § 【当前时间】：显示系统当前的时间。
- § 【系统时间设置】：手动设置/时间服务器。
- § 【日期设置】：设置系统的日期。
- § 【时间设置】：设置系统的时间。

p 同步时间设置

NTP即网络时钟协议，即通过本地主机和网络时钟服务器进行自动对时（时间同步），进入“系统”
à “系统时间”，看到如下图时间服务器配置界面：



系统时间

当前时间	2011年05月02日,22:43:32	
系统时间设置	时间服务器	
同步间隔	60	范围:15~65535 单位:秒
时间服务器	time.windows.com *	

取消

保存

图4-2. NTP配置界面

- § 【同步间隔】：设置时间同步时的间隔值。
- § 【时间服务器】：指定网络上提供时钟对时服务的服务器域名或IP地址。

% 注意：
NTP服务器不一定为Internet上的服务器，但必须是MP1800-20路由器能够访问到的服务器。

4.1.2 远程日志

系统可发送设备日志信息到远程日志服务器。进入“系统” à “远程日志”，看到如下配置界面：

远程日志

启用	☐
远程日志服务器IP地址	*

取消

保存

图4-3. 远程日志配置界面

- § 【启用】：是否发送设备日志信息到远程日志服务器。
- § 【远程日志服务器IP地址】：配置远程日志服务器的IP地址。



4.1.3 管理控制

MP1800-20路由器的管理控制功能可以控制系统是否启用SSH服务、Telnet服务或HTTP服务，进入“系统” à “管理控制”，看到如下配置界面：

管理控制

启用SSH	☒
启用远程SSH	☒
启用Telnet	☐
启用远程HTTP	☒

✖ 取消

✔ 保存

图4-4. 管理控制配置界面

4.1.4 配置管理

MP1800-20路由器的配置管理功能提供对用户配置的备份与恢复。“备份”可将系统已配好的参数信息保存至PC机上，以备需要时使用；“恢复”可将所保存的配置参数恢复到系统中。

备份配置

进入“系统” à “配置管理”，看到如下界面：

配置管理

选择上传文件：

浏览...

恢复

备份

恢复出厂设置

图4-5. 备份配置界面

点击“备份”按钮即可备份当前系统的用户配置。

% 注意：
请将备份文件保存至便于您获取的、较为安全的主机磁盘中，以免丢失。



p 恢复配置

当您需要将用户配置恢复到系统时，进入“系统”à“配置管理”，点击浏览选择保存的备份文件，然后点击“恢复”。如下图：

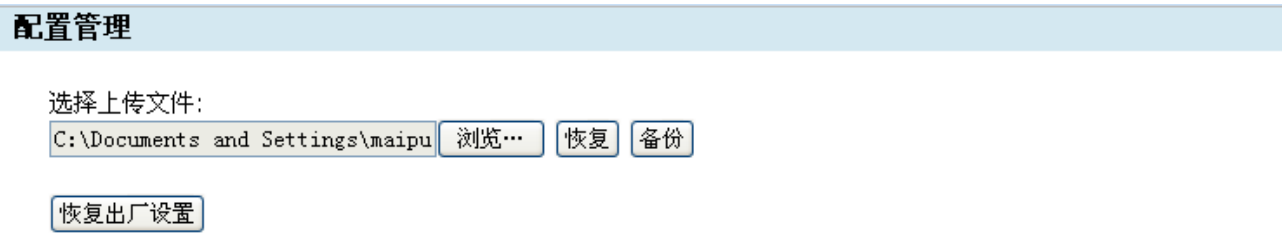


图4-6. 恢复配置

p 恢复出厂设置

当您需要将系统恢复至出厂状态时，进入“系统”à“配置管理”，点击“恢复出厂设置”即可。

4.1.5 系统升级

MP1800-20路由器可进行远程Web升级，在升级之前请您确定您已获得系统更新的目标文件。升级时进入“系统”à“系统升级”，看到如下界面：

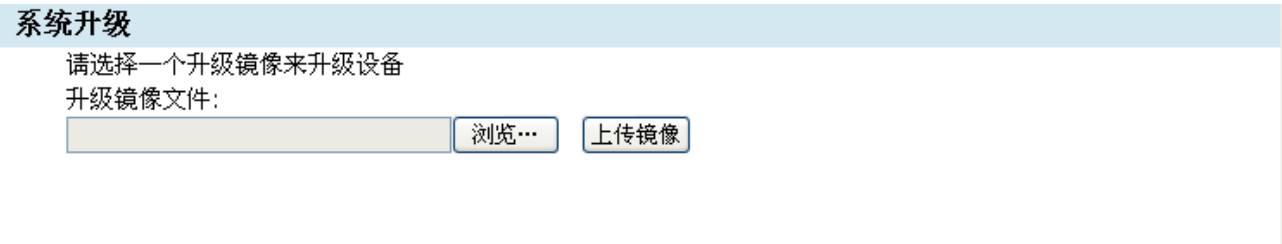


图4-7. 系统升级界面

点击“浏览”查找到目标文件，点击“上传镜像”系统开始上传镜像，上传完成后如下图：

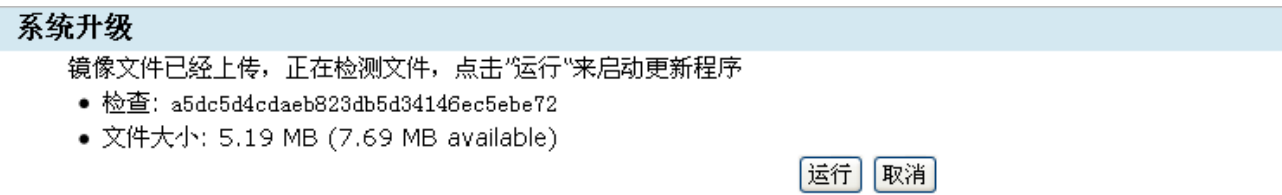


图4-8. 升级过程



点击“运行”开始升级系统。升级过程比较慢，可以通过升级进度条来查看升级进度。当升级成功后，页面会自动跳转到登录页面。

4.1.6 SNMP

当您想要配置SNMP时，进入“系统” à “SNMP”，看到如下界面：

SNMP配置

启用

☐

系统位置

maipu

*

联系人

admin@maipu.co

*

系统名称

3GRouter

*

系统描述

3GRouter

*

团体名

public

取消

保存

图4-9. SNMP配置界面

- § 【启用】：是否启用SNMP。
- § 【系统位置】：填写本路由器所处的位置。
- § 【联系人】：填写本路由器的管理员的联系方式。
- § 【系统名称】：填写本路由器的名称。
- § 【系统描述】：填写本路由器的描述。
- § 【团体名】：指定SNMP的团体名。

& 提示：
以上的配置都会被设置到MIB（管理信息库）相应的节点中。

4.1.7 修改密码

MP1800-20路由器提供更改用户密码的权限，进入“系统” à “修改密码”，可以为系统管理员admin设置新的密码，如下图：



修改密码

旧密码		* 最短4位，最长16位
新密码		* 最短4位，最长16位
确认密码		* 最短4位，最长16位

复位

提交

图4-10. 修改密码

4.1.8 重启系统

当您想要通过软件来重启MP1800-20路由器时，进入“系统”à“重启系统”，看到如下界面，点击“重启”按钮即可。

重启系统

点击重启按钮，重新启动系统

重启

图4-11. 系统重启界面

% 注意：
重启执行成功后，需要重新登录系统才能配置！

4.1.9 退出登录

当您想要退出MP1800-20路由器网页配置界面时，进入“系统”à“退出登录”即可。

4.2 网络

MP1800-20路由器网络设置包括以下功能：



- n 拨号接口
- n LAN接口
- n 转发模式
- n 动态域名
- n 静态路由
- n 动态路由

4.2.1 拨号接口

1) 基本设置

进入“网络” à “拨号接口” à “基本设置”，看到移动网络基本配置界面：

基本设置

网络提供商	中国联通
网络模式	自动切换
接入点	3gnet *
用户名	wcdma *
密码	***** *
PIN 码	
启用SIM卡绑定	☐

取消

保存

图4-12. 移动网络基本设置

- § 【网络提供商】：显示网络提供商，中国联通/中国电信。
- § 【网络模式】：设置移动网络接入方式（2.5G/3G/自动切换）。
- § 【接入点】：设置拨号时所使用的接入点（可从网络提供商处获得，电信设备无该配置选项），最大长度32位。
- § 【用户名】：设置拨号时所使用的用户名（可从网络提供商处获得），最大长度32位。
- § 【密码】：设置拨号时所使用的密码（可从网络提供商处获得），最大长度32位。
- § 【PIN码】：设置SIM卡PIN密码，最大长度8位。



§ 【启用SIM卡绑定】：设置SIM卡绑定功能。若启用此项，则将SIM卡的IMSI码与系统绑定，当第一次使用3G模块时记录该卡号，后续如果使用其他卡并且启用此项则出错。

对于普通用户，以上基本参数配置完成并保存后，MP1800-20路由器就会在每次加电后自动进行无线网络拨号连接，使用极其方便。

2) 链路类型

设置链路连接方式，可以选择为“永久在线”或者“按需拨号”两种，进入“网络”à“拨号接口”à“链路类型”，看到链路类型配置界面：

链路类型

永久在线

取消 保存

图4-13. 永久在线

§ 【永久在线】：使网络连接一直处于在线状态。

链路类型

按需拨号

空闲间隙 120 * 范围:0~2147483647 单位: 秒

取消 保存

图4-14. 按需拨号

§ 【按需拨号】：当有业务数据流时才会触发拨号。

§ 【空闲间隙】：设置连接空闲时间，达到空闲时间后关闭连接。

3) 高级设置

如果您是高级用户，那么您进入“网络”à“拨号接口”à“高级设置”，可以继续选择完成下面的高级参数配置：

1. 认证和加密参数：



高级设置

CHAP状态	自动协商 ▼
PAP状态	自动协商 ▼
MS-CHAP状态	自动协商 ▼
MS2-CHAP状态	自动协商 ▼
EAP状态	自动协商 ▼

图4-15. 认证&加密参数

- § 【CHAP】：挑战握手协议（Challenge-Handshake Authentication Protocol），是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。主要针对PPP的，认证时密钥信息不需要在通信信道中发送，而且每次认证所交换的信息都不一样，可以很有效地避免监听攻击，安全性较高。
- § 【PAP】：是一种简单的明文验证方式，要求将密钥信息在通信信道中明文传输，因此容易被sniffer监听而泄漏。
- § 【MS-CHAP】：与CHAP相类似，MS-CHAP也是一种加密验证机制，使用基于MPPE的数据加密。
- § 【MS2-CHAP】：MS-CHAP版本2。
- § 【EAP】：是一种可扩展认证协议，该协议用于在PPP等点到点网络中的认证，可支持多种认证机制。使用可扩展认证协议，任意身份验证机制都可以对远程访问连接进行身份验证。

2. 压缩和控制协议参数

压缩控制协议	拒绝 ▼
地址-控制压缩	拒绝 ▼
协议域压缩	拒绝 ▼
VJ TCP/IP 头部压缩	拒绝 ▼
连接ID压缩	拒绝 ▼

图4-16. 压缩 & 控制协议



- § 【压缩控制协议】：负责在PPP链路上的两端配置并协商采用哪种压缩算法。并且用可靠的方式来标志压缩和解压缩机制的失败。
- § 【地址/控制压缩】：是否允许进行IP地址和控制压缩设置。
- § 【协议域压缩】：是否启用协议域压缩。
- § 【VJ TCP/IP头部压缩】：是否允许TCP/IP数据报进行Van Jacobson头部压缩。
- § 【连接ID压缩】：是否允许进行连接ID压缩。

3. 其他参数

其他参数设置提供您是否允许使用对端DNS、LCP回显间隔、LCP回显失败、数据报大小处理以及调试IP的设置。

调试	启用
使用对端DNS	启用
识别无效DNS	☐
LCP回显间隔	10 * 范围:1~2147483647 单位: 秒
LCP回显失败	6 * 范围:1~2147483647
最大传输单元	1500 * 范围:128~16384
最大接收单元	1500 * 范围:128~16384
本地IP	
远端IP	

取消

保存

图4-17. 杂项

- § 【使用对端DNS】：是否允许使用对端DNS，默认为“启用”。
- § 【识别无效DNS】：勾选则检测获取的DNS是否有效。若无效，则重新拨号。
- § 【LCP回显间隔】：PPP链路控制协议（LCP）回显间隔设置，设置范围：1~2147483647。
- § 【LCP回显失败】：PPP链路控制协议（LCP）回显失败次数设置，设置范围：1~2147483647。
- § 【最大传输单元】：允许MP1800-20路由器在PPP链路上的最大传输数据报大小设置，以字节为单位，对于局域网来说，最大传输单元的值一般是 1,500 字节，PPP链路传输的最大数据报大小可以设置稍小。
- § 【最大接收单元】：允许MP1800-20路由器接收到的最大传输数据报大小设置。
- § 【本地IP】：设置MP1800-20路由器在3G拨号时，进行PPP IPCP协商时的本地IP。



§ **【远端IP】**：设置MP1800-20路由器在3G拨号时，进行PPP IPCP协商时的对端IP。

4.2.2 LAN接口

LAN接口配置项提供您对MP1800-20路由器以太网口的配置。进入“网络” à “LAN接口”，看到如下配置界面：

The screenshot shows the 'LAN接口' (LAN Interface) configuration page. It contains two input fields: 'IP 地址' (IP Address) with the value '192.168.10.1' and '子网掩码' (Subnet Mask) with the value '255.255.255.0'. Both fields have a red asterisk icon to their right. At the bottom right, there are two buttons: '取消' (Cancel) with a red 'X' icon and '保存' (Save) with a green checkmark icon.

图4-18. LAN设置

§ **【IP地址】**：设置或修改MP1800-20路由器LAN IP地址，默认为：192.168.10.1。一般为直连计算机的网关IP或者局域网网关。

§ **【子网掩码】**：设置或修改用于标识LAN IP所在的网络地址的特殊IP地址，如：255.255.255.0。

& 提示：

1. 如果您无需修改MP1800-20路由器LAN IP，那么可以跳过LAN设置。
2. 如果您修改了MP1800-20路由器LAN IP出厂值，那么请您返回第三章3.3节重新配置计算机，并重新登录MP1800-20路由器。

4.2.3 转发模式

转发模式用于设置数据包的转发方式是基于路由查找或IP地址伪装。进入“网络” à “转发模式”，看到如下配置界面：



图4-19. 转发模式设置

- § 【路由模式】：通过查找系统路由表决定数据包的转发路径。
- § 【NAT模式】：对数据包做源地址伪装实现局域网共享一个IP上网的需求。

% 注意：
一般在拨号上网的应用环境中转发模式推荐设置为“NAT模式”，这样可以减少对路由表的配置。

4.2.4 动态域名

DDNS(dynamic domain system)是动态域名系统的缩写，DDNS协议提供动态IP和域名之间的对应查询功能。使用MP1800-20路由器，您可以快速方便的访问局域网内部映射到动态IP上的服务。

进入“网络” à “动态域名”，看到如下配置界面：

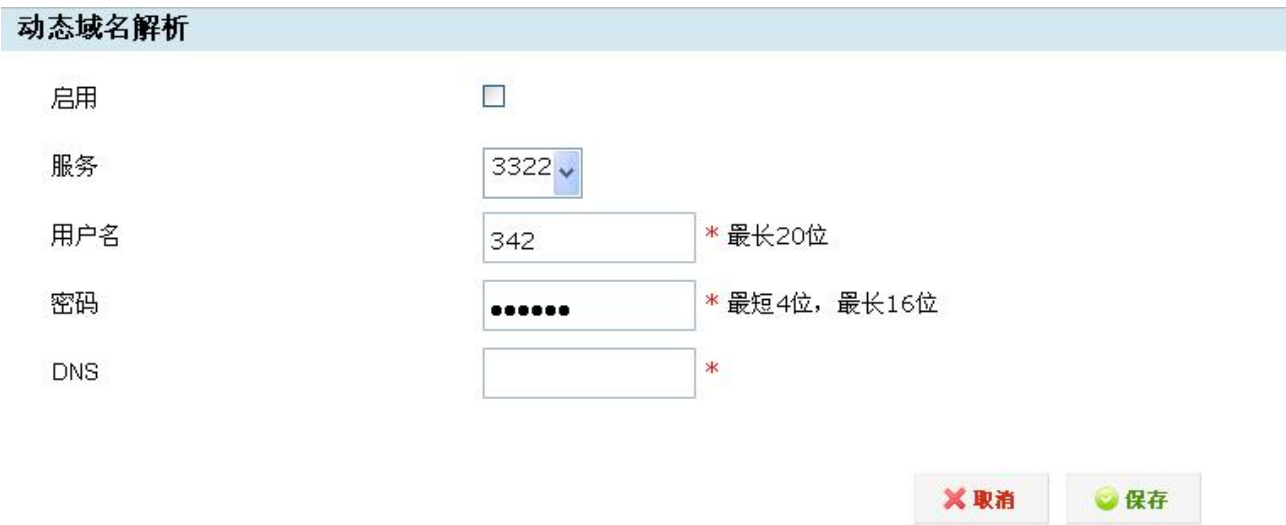


图4-20. 动态域名配置界面

- § 【启用】：使能开关，勾选则激活DDNS，否则禁用DDNS。



- § 【服务】：DDNS服务选择，目前只支持3322。
- § 【用户名】：在DDNS服务提供商处申请的用户名。
- § 【密码】：在DDNS服务提供商处申请的密码。
- § 【DNS】：在DDNS服务提供商处设定的DNS域名。

4.2.5 静态路由

静态路由表能为向外发送的数据报确定外出路由，当MP1800-20路由器网络与目标访问网络有多个路由器或子网，就需要设置静态路由器来使不同的子网之间能相互通信。

进入“网络” à “静态路由”，看到如下配置界面：

静态路由

目标	子网掩码	网关	接口	
192.168.0.0	255.255.255.0	10.10.10.1	LAN	
增加				
				取消 保存

图4-21. 静态路由添加配置界面

- § 【目的 IP】：设置静态路由的目标地址，如192.168.0.1
- § 【子网掩码】：设置子网掩码。
- § 【网关】：设置静态路由的下一跳IP地址，即相邻路由器的端口地址。
- § 【接口】：指定静态路由所作用的接口。

点击图标 可用删除对应静态路由。

% 注意：

1. 增加路由信息后，必须点击“保存”使设备生效，点击“保存”前，请不要切换到其它页面。
2. 当目的地址设置为某一个具体IP时，子网掩码必须设置为255.255.255.255。否则系统会自动根据子网掩码计算出一个网络地址。
3. 如果还想添加路由信息，那么请点击增加按钮。
4. 加按钮继续添加静态路由。

4.2.6 动态路由

MP1800-20路由器支持RIP动态路由，进入“网络” à “动态路由”可以进行RIP动态路由的配置。如下图所示：



1、动态路由

动态路由

启用	☐
版本	2
接收V1报文	☐
源地址检测	☐
更新周期	30 * 范围:5~2147483 单位: 秒
失效时间	180 * 范围:5~2147483 单位: 秒
锁定时间	180 * 范围:0~2147483 单位: 秒
刷新时间	240 * 范围:5~2147483 单位: 秒
发布路由	☐ LAN ☐ 拨号接口 ☐ GRE隧道:maipugre

图4-22. 动态路由配置页面

- § 【启用】：是否启用RIP服务。
- § 【版本】：选择RIP的版本，分别是RIPv1和RIPv2。
- § 【接收V1报文】：当选择RIPv2时，选择是否接收RIPv1的报文。
- § 【源地址检测】：选择是否检测点对点接口的源地址，默认是关闭的。
- § 【更新周期】：RIP路由更新时间，发送路由信息的时间间隔。
- § 【失效时间】：设置路由信息为失效的时间间隔，超过该时间未收到更新报文，则将路由信息置为不可达，但是不清除路由信息。
- § 【锁定时间】：设置路由信息的锁定时间，锁定时间主要是为了防止路由环路的。
- § 【刷新时间】：清除路由信息的时间，路由条目进入无效状态时启动刷新计时器，超过该时间未收到更新报文，则清除相关路由信息。
- § 【发布路由】：勾选想要发布出去的接口。如果不勾选，则该接口不会发送和接收路由更新信息。

2、邻居

进入“网络” à “动态路由”如下界面：



图4-23. 邻居节点配置页面

§ 【邻居】：设置RIP路由的邻居节点，RIP每次更新路由信息时，会以单播的方式发送更新到该主机。

% 注意：

- 1. 增加邻居信息后，必须点击“保存”使设备生效，点击“保存”前，请不要切换到其它页面。

4.3 服务

MP1800-20路由器的服务功能包括：

- n DHCP设置
- n 热备份

4.3.1 DHCP设置

1、DHCP服务器

DHCP（Dynamic Host Configuration Protocol）动态主机地址分配协议，主要用于给网络主机分配动态的IP地址，从而使得繁琐的手动配置过程变得简单轻松，特别是较大局域网的IP配置，使用DHCP服务可以为网络管理人员大大的降低工作量。

MP1800-20路由器内置DHCP服务器，让它为您的局域网提供动态IP分配服务。进入“服务”à“DHCP设置”，看到如下配置界面：



DHCP设置

DHCP服务	☒
DHCP网络地址	192.168.10.0
起始地址	192.168.10.100 *
结束地址	192.168.10.250 *
有效时间	10h * 格式: 数字加上单位(h,m,s) 如:12h

图4-24. DHCP设置界面

§ 【DHCP服务】：使能开关，勾选则启用DHCP服务，否则禁用DHCP服务。

§ 【起始地址】：设置的起始地址必须与LAN口IP地址在同一个网络中，不能为广播地址或LAN口地址。

§ 【结束地址】：设置的结束地址必须与LAN口IP地址在同一个网络中，不能为广播地址或LAN口地址。

§ 【有效时间】：设置一个IP地址的保持时间，最小值为2分钟，单位为h或m或s。

& 提示：

DHCP服务应用时，要求开启客户端主机的“自动获取IP地址”的功能。

对于其他类型的客户端设备的“自动获取IP地址”功能开启，请参考该设备的使用说明。

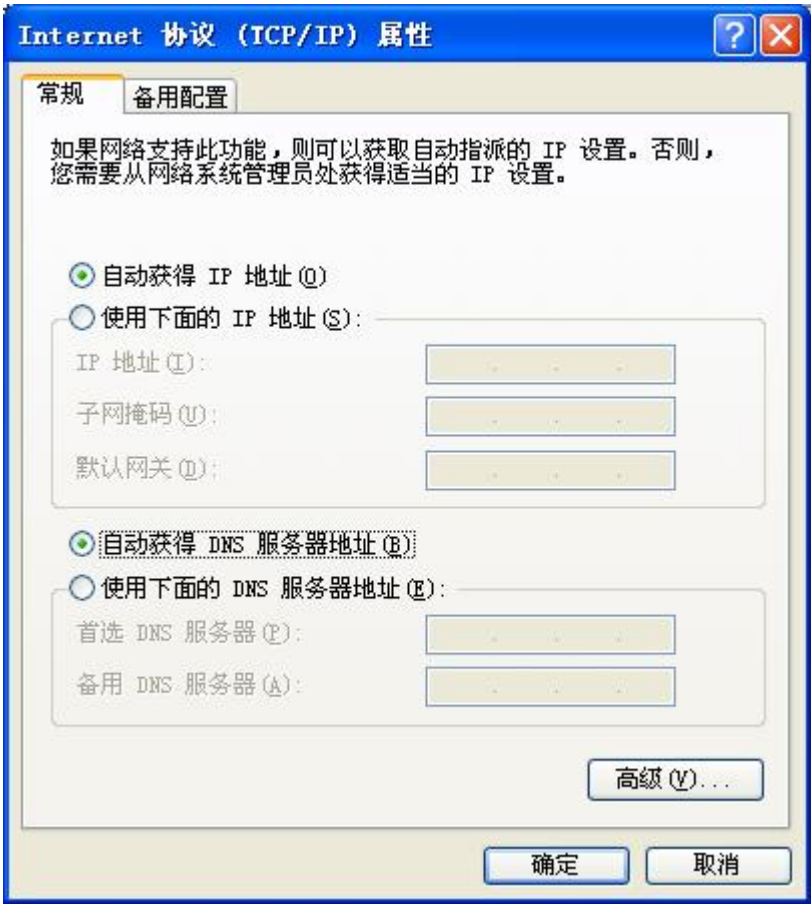


图4-25. 自动获得IP地址设置

2、静态IP映射

“静态IP映射”即IP-MAC映射设置，通俗说就是进行IP地址和MAC地址的绑定设置。您可以事先通过把IP地址与网络设备的网卡物理地址（MAC）捆绑起来的方式为局域网设备分配IP地址，以供联网，这样不但节省工作时间，还可以起到保护局域网不受某些病毒（如ARP欺骗等）的影响。

进入“服务”à“DHCP设置”如下界面：



静态IP映射

MAC	IP
增加	X

图4-26. 自动获得IP地址设置

§ **【MAC】**：设置静态IP主机的MAC地址。如：00:50:56:C0:00:08。

§ **【IP】**：设置分配的静态IP地址，该IP地址必须与LAN口IP地址在同一个网络中，不能为广播地址或LAN口地址。

% 注意：

1. 增加静态IP映射信息后，必须点击“保存”使设备生效，点击“保存”前，请不要切换到其它页面。

& 提示：

“静态IP映射”同样要求客户端主机开启“自动获取IP地址”功能。

4.3.2 热备份

“热备份”是指当前MP1800-20路由器遇到死机等情况时，可以直接转到备份路由器，从而继续进行正常工作。

进入“服务”à“热备份”，看到如下配置界面：



热备份

启用

☐

接口

LAN

域间同步接口

LAN

优先级

100

* 范围: 1~254

保活时间

1

* 范围: 1~255 单位: 秒

认证类型

PASS

认证密码

* 最大长度为8

虚拟IP

*

取消

保存

图4-27. 热备份配置界面

- § 【启用】：是否启用vrrp功能。
- § 【接口】：负载均衡工作接口（一般设置为lan口）。
- § 【域间同步接口】：vrrp广播报文的通信接口（一般设置为lan口）。
- § 【优先级】：优先级最高的为将成为主路由器在工作。
- § 【保活时间】：vrrp报文发送周期，缺省设置为1秒。
- § 【认证类型】：主路由器与备份路由器（组）之间的交互报文的认证方式，主、备路由器（组）之间的设置必须一致（PASS为未加密的明文认证方式/AH为加密认证方式）
- § 【认证密码】：主、备路由器（组）之间的设置必须一致。
- § 【虚拟IP】：主、备路由器（组）对外提供的虚拟IP地址，作为终端的默认服务网关（主、备路由器（组）之间的设置必须一致）。

4.4 状态防火墙

MP1800-20路由器的“状态防火墙”功能包括：

- n 基本设置
- n 访问控制
- n 端口映射



n MAC-IP绑定

4.4.1 基本设置

基本设置用来设置当前MP1800-20路由器防火墙的默认动作，包括防火墙默认处理策略，是否过滤来自Internet的Ping包，是否防止Dos攻击，是否开启状态防火墙。进入“状态防火墙” à “基本设置” 设置界面：

基本设置

默认处理策略	放行
防止Dos攻击	☒
状态防火墙	☒
过滤来自Internet的Ping包	☒
TCP MSS设置方式	手动设置
TCP MSS值	1460 * 范围:500~1460

取消

保存

图4-28. 基本设置

- § 【默认处理策略】：设置防火墙的默认动作。经防火墙转发的数据包如果没有匹配任何一条有效的规则，最后便会执行此默认处理动作。
- § 【过滤来自Internet的Ping包】：选中状态为开启，开启时将过滤外部的ping报文。
- § 【TCP MSS设置方式】：可选择自动设置和手动设置方式。
- § 【TCP MSS值】：手动设置TCP MSS的值。范围：500~1460。
- § 【防止Dos攻击】：开启时可以一定程度上防止来自外部的Dos攻击。
- § 【状态防火墙】：选中状态为开启。开启状态下可以过滤无效的数据包。

4.4.2 访问控制

防火墙安全控制是通过添加的安全规则来实现的，想要实现某种IP过滤控制，您必须向MP1800-20路由器IP过滤规则库添加相应的控制规则，才能达到您使用MP1800-20进行安全控制保护的目的。进入“状态防火墙” à “访问控制”，如下配置界面：



访问控制

启用	☐
协议	TCP
源接口	LAN
源IP地址	
源端口	
目的接口	拨号接口
目的IP地址	
目的端口	
动作	接受
返回访问控制列表	



图4-29. 访问控制

- § 【启用】：选中状态将启用这条规则。
- § 【协议】：可以为tcp协议，udp协议，icmp协议或者同时指定tcp和udp协议。
- § 【源IP地址】：一般为内网的PC的IP或者网段，如：192.168.10.0/24。
- § 【源端口】：可以为区段，如：22-8888。在您不确定源端口的情况，此项最好不要填写。
- § 【目地IP地址】：可以为区段，同源IP地址。
- § 【目地端口】：可以为区段，同源端口。
- § 【动作】：指定规则对数据包的处理方式（接受/拒绝/丢弃）。

点击图标 可用删除对应规则。

& 小技巧:

如果您想要禁止局域网访问大部分Internet服务时，你可以按照下面的思路进行添加设置

第一步：禁止对所有Internet服务的访问。

第二步：开放例外的服务。

说明：防火墙的所有规则都遵循“晚配置，早匹配”的原则。



4.4.3 端口映射

使用MP1800-20路由器网络端口映射(NAT)功能，允许您进行Internet公网IP地址与内部私有IP地址一对一映射。进入“状态防火墙” à “端口映射”，看到如下配置界面：

端口映射

启用	协议	源端口	目的IP地址	目的端口	
☐	TCP				
增加					
				取消	保存

图4-30. 端口映射

- § 【启用】：选中状态为启用。
- § 【协议】：可以为tcp, udp，或者同时指定两者。
- § 【源端口】：为某一特定整数。表示所要映射的源端口号。
- § 【目地IP地址】：为内网某一PC的IP。表示所要映射的目的主机的IP地址。
- § 【目地端口】：目地IP的某一端口。所要映射的目的端口号。

点击图标 可用删除对应端口映射。

% 注意：

1. 增加端口映射信息后，必须点击“保存”使设备生效；点击“保存”前，请不要切换到其它页面。

4.4.4 MAC-IP绑定

MAC-IP绑定该功能用于限定局域网内对指定IP地址的主机根据其IP和MAC同时匹配的方式对数据包进行过滤，可选的过滤方式为接受、拒绝或丢弃。



MAC-IP绑定

启用	☐
IP 地址	
物理地址	
动作	接受 v

[返回MAC-IP绑定列表](#)

✕ 取消

✔ 保存

图4-31. MAC-IP绑定

§ 【IP地址】：局域网中某台主机的实际、有效的合法IP地址，例如：192.168.10.11。

§ 【物理地址】：局域网计算机MAC地址，如MAC：00:50:56:C0:00:08。

§ 【动作】：即指定处理动作，可以为接受、拒绝或丢弃。

点击图标  可用删除对应MAC-IP绑定。

4.5 QOS

MP1800-20路由器QOS包括：

n 带宽管理

4.5.1 带宽管理

进入“QOS” à “带宽管理”，选中“启用状态”，可设置下载速度和上传速度。如下图：



带宽管理

启用	☒	
下载速度	1024	* 范围:1~15000 单位:kbps
上传速度	128	* 范围:1~15000 单位:kbps

图4-32. 带宽管理

- § 【启用状态】：可以设置为启用状态或则关闭状态。设置为启用之后可以指定上传和下载的速率。
- § 【下载速度(kbps)】：指定下载速度(单位kbps)。
- § 【上传速度(kbps)】：指定上传速度(单位kbps)。

4.6 VPN配置

VPN（Virtual Private Network）虚拟专用网缩写，是基于Internet的一种安全局域网，目前MP1800-20路由器支持IPSec、L2TP和GRE三种协议，为企业网络安全提供了灵活而经济有效的方案选择。

MP1800-20路由器的“VPN配置”功能包括：

- n IPSEC
- n L2TP
- n GRE
- n 证书管理

4.6.1 IPSec

IPSec是IP安全协议（IP Secure Protocol）英文缩写，是VPN技术的一种，该协议不但涉及数据封装和加解密技术，还涉及数据的传输和验证技术。常用于端对端的网络安全传输！

(一) IPSEC隧道配置

进入“VPN” à “IPSec” à “配置隧道”便可以进入IPSEC配置界面,如下图：



IPSec隧道配置

第一阶段标识	启用	远端网关	本地子网	远端网络
尚未设置				
请输入第一阶段标识				
增加				

图4-33. IPSec隧道管理

§ 【隧道名称】：第一阶段标识：为您建立的IPSec隧道设立一个名称以方便查看。

% 注意：

1. 修改VPN隧道配置时，第一阶段标识不可以修改。
2. MP1800-20路由器的IPSec服务缺省为禁用状态，要使所创建的所有规则生效，在开启某条规则状态时，还必须注意开启该服务。
3. IPSec隧道配置分为两个阶段，第一阶段和第二阶段。

1 添加规则

在图4-32界面输入完隧道名称后，点击“增加”进入IPSec隧道参数配置界面，如下图。

1) 基本配置



第一阶段配置

第一阶段标识	tun1
启用	☐
NAT穿越	☐
DPD间隔	30 * 范围:0~3600 单位: 秒
DPD最大重传次数	5 * 范围:1~100
远端网关	*
认证模式	预共享密钥 ▾
协商模式	主模式 ▾
本地ID类型	地址 ▾
本地ID数值	*
辨别对端ID	☐
加密算法	DES ▾
认证算法	MD5 ▾
密钥组	GROUP1 ▾
生命周期	86400 * 范围:0~31536000 单位: 秒

[返回第一阶段配置列表](#)

第二阶段配置

本地网络	本地掩码	远端网络	远端掩码	隧道模式	PFS群组	生命周期
尚未设置						

图4-34. IPSec第一阶段基本配置



第一阶段配置：

§ 【启用】：IPSec隧道使能开关。缺省为禁用状态，勾选为启用。

§ 【NAT穿越】：为了防止NAT网关对IPSec隧道的的影响，推荐启用NAT穿越（隧道数据可以穿越NAT网关）。

§ 【DPD间隔】：安全隧道对端状态探测间隔（描述：每隔一段DPD间隔时间，IPSEC会发送一个DPD探测数据包，用来判断隧道对端是否存活，如果对端无回应，IPSEC会发起重协商）。

§ DPD最大重传次数：设置安全隧道对端状态探测的最大重传次数。

§ 【远端网关】：远端网关地址（一般为远端公网IP地址）。

§ 【认证模式】：可以选择预共享密钥或者数字证书。一般选择为预共享密钥。

§ 【中心证书名】：选择认证中心的证书。（CA证书）。该证书需要在证书上传配置项里上传相应证书。（该选项依赖于认证模式为数字证书和本地ID类型为ASD1DN。）

§ 【证书内容】：选择数字证书。该证书需要在证书上传配置项里上传相应证书。（该选项依赖于认证模式为数字证书和本地ID类型为ASD1DN。）

§ 【证书私钥】：选择数字证书对应的私钥。该证书需要在证书上传配置项里上传相应证书。或者在证书申请里面获得。（该选项依赖于认证模式为数字证书和本地ID类型为ASD1DN。）

§ 【协商模式】：可以选择为主模式、积极模式。一般选择主模式。

§ 【本地ID类型】：可以选择地址、FQDN、USER_FQDN、ASD1DN。

§ 【本地ID数值】：可根据选择的本地ID类型填入相应标志。填写方法由本地ID类型决定。当其中选择IP地址则填写本机IP地址，选择FQDN或者USER_FQDN时，可以填写字符串，选择ASD1DN时，不会出现该项，ASD1DN主要用于数字证书。

§ 【辨别对端ID】：可勾选上表示需要辨别对端ID。

§ 【加密算法】：IPSec第一阶段使用的加密算法，可以选择为DES、3DES、blowfish、aes。默认为SM1（针对SJW12-C-AC或者SJW12-W-AC）或DES（针对RM1800-20C或者RM1800-20W）。

§ 【认证算法】：IPSec第一阶段使用的认证算法，可以选择为MD5、SHA1、SHA256。默认为MD5。

§ 【密钥组】：选择需要的密钥组（该密钥组也是DH算法）。

§ 【生命周期】：IPSec第一阶段生命周期。



第二阶段配置

本地网络	192.168.10.0	*
本地掩码	24	
远端网络		*
远端掩码	24	
隧道模式	ESP	
加密算法	DES	
认证算法	MD5	
PFS群组	OFF	
生命周期	28800	* 范围:0~31536000 单位: 秒

[返回第二阶段配置列表](#)

图4-35. IPSec第二阶段基本配置

第二阶段配置：

本地子网

- § 【本地网络】：IPSec本地保护子网。例如：192.168.10.0。
- § 【本地掩码】：IPSec本地保护子网掩码。例如：255.255.255.0，则选择24。
- § 【远端网络】：IPSec远端保护子网。例如：192.168.20.0。（网络号或者单台主机，由对端IPSEC隧道配置决定）
- § 【远端掩码】：IPSec远端保护子网掩码。例如： 255.255.255.0，则选择24。
- § 【隧道模式】：可以选择为ESP协议，AH协议一般使用ESP协议。
- § 【加密算法】：IPSec第二阶段使用的加密算法，可以选择为SM1、DES和3DES、BLOWFISH、AES128、AES192、AES256、NULL。默认为SM1（针对SJW12-C-AC或者SJW12-W-AC）或DES（针对RM1800-20C或者RM1800-20W）。
- § 【认证算法】：IPSec第二阶段使用的认证算法，可以选择为MD5和SHA1、SHA2-256、NULL等。默认为MD5。
- § 【PFS群组】：完美前向加密（DH算法），可以选择为off、768bit、1024bit、1536bit。此参数需要跟对端匹配。
- § 【生命周期】：IPSec第二阶段生命周期。当生命周期结束后，IPSEC会发起第二阶段参数重协商。

2) 预共享密钥配置



IPSec预共享密钥配置

对端ID	密钥
尚未设置	
	
 	

图4-36. 预共享密钥设置

在上图中点击“增加”按钮以后，进下面配置预共享密钥界面，如下图：

IPSec预共享密钥配置

对端ID	密钥
	
	
 	

图4-37. 预共享密钥

- § 【对端ID】：对端ID数值（可以是字符串，IP地址，域名）。
- § 【密钥】：用于填写预共享密钥。

点击图标  可用删除对应的密钥。

% 注意：

1. 增加IPSec预共享密钥配置信息后，必须点击“保存”使设备生效，点击“保存”前，请不要切换到其它页面。

3) 高级设置



高级设置

IPSec预分片☒

SM1使用SCB2兼容方式☒

取消

保存

图4-38. 高级设置

- § 【IPSec预分片】：勾选开启IPSec预分片功能。
- § 【SM1使用SCB2兼容方式】：勾选开启SM1使用SCB2兼容方式功能。

2 修改IPSEC隧道配置

当要修改某条IPSec隧道配置时，进入“VPN” à “IPSec” à “配置隧道”便可用进入IPSec隧道配置界面，如下图：

IPSec隧道配置

第一阶段标识	启用	远端网关	本地子网	远端网络	
fff	启用	192.168.30.1	192.168.10.0/24	192.168.30.0/24	 

请输入第一阶段标识

增加

图4-39. IPSec规则修改

在上图中的已建隧道一栏点击“”便可以进入IPSec 隧道配置编辑界面，如图4-39:

详细参数说明不在赘述，如需了解请参考规则添加部分内容。

3 查看隧道状态

进入“状态” à “隧道状态”便可以查看当前IPSec隧道的连接状态，如下图：



IPSec隧道状态

刷新

隧道SA信息

隧道#1:(192.168.10.0/24[any])182.144.176.250 <-> 119.6.69.212 (100.100.100.0/24[any])
封装:esp,des-cbc,hmac-md5,Tunnel,SPI: 0xcdbf027b/0x0c2a7ddb
接收流量:1020(bytes)/13(packets)
发送流量:1696(bytes)/13(packets)
生命周期:28800(s)
运行时间:0 天0 小时8 分27 秒

当前隧道总数:1

图4-40. 隧道连接状态

- § 【SA】：IPSec安全关联。
- § 【隧道】：显示隧道两端的网关地址。
- § 【封装】：显示隧道的安全协议，如esp, ah等；加密算法-认证算法-协商模式（Transport或Tunnel）；两个方向的安全关联的spi（安全参数索引）值。
- § 【接收流量】：通过隧道，接收到对端发来的数据流量。
- § 【发送流量】：通过隧道，发送到对端的数据流量。
- § 【生命周期】：IPSec sa的最大使用时间。
- § 【运行时间】：隧道建立的时间长度。
- § 【当前隧道总数】：设备中已经建立的隧道总数。

4 删除规则

当不需要某条IPSec隧道配置时，通过图4-38中隧道一栏点击“”即可删除相应的IPSEC隧道。

4.6.2 L2TP

L2TP（Layer Two Tunneling Protocol）第二层通道协议的缩写，它是VPDN（虚拟专用拨号网络）技术的一种，专门用来进行第二层数据的通道传送，L2TP提供了一种远程接入访问控制的手段，其典型的应用场景是：某公司员工通过 PPP拨入公司本地的网络访问服务器（NAS），以此接入公司内部网络，获取IP地址并访问相应权限的网络资源。该员工拨入公司网络如同在公司局域网一样安全方便。

进入“VPN” à “L2TP”，看到如下配置界面：



L2TP隧道配置

隧道名称	启用	服务器	用户名	密码
尚未设置				

输入隧道名称,添加隧道:

增加

图4-41. VPN隧道管理界面

【隧道名称】：L2TP隧道名称设置，建议采用易于识别的名称。如城市-城市、特定事件（出差）等等。

% 注意：
修改VPN隧道配置时，隧道名称不可以修改。

1. 添加新规则

填好隧道名称后，如图4-41，点击“增加”开始设置L2TP隧道，如下图：

L2TP隧道配置

隧道名称: netb

启用 ☒

服务器 *

用户名 *

密码 *

[返回L2TP列表](#)

取消 保存

图4-42. 添加L2TP连接

§ 【启用】：勾选则启用该L2TP隧道。



- § 【服务器】：L2TP服务器地址。
- § 【用户名】：建立L2TP隧道，在服务器上认证的用户名。
- § 【密码】：建立L2TP隧道，在服务器上认证的密码。

2. 修改隧道配置



图4-43. 修改隧道配置

当要修改某条已配置好的隧道，在上图中在对应规则行点击“”就可以修改。修改的配置界面同图4-42。

3. 删除规则

如果长期不使用某条隧道，或者不需要某条隧道，我们建议您删除，进入上图4-43界面，找到要被删除的隧道，点击“”即可删除。

4.6.3 GRE

GRE(通用路由协议封装)规定了如何用一种网络协议去封装另一种网络协议的方法。GRE协议的主要用途有两个：企业内部协议封装和私有地址封装。在国内，由于企业网几乎全部采用的是TCP/IP协议，因此在中国建立隧道时没有对企业内部协议封装的市场需求。企业使用GRE的唯一理由应该是对内部地址的封装。

进入“VPN” à “GRE”便可以进入GRE 隧道配置编辑界面，如下图：



GRE隧道配置

GRE隧道名称	启用	对端外网IP	对端内网IP	对端内网掩码
尚未设置				
输入隧道名称,添加隧道:				
增加				

图4-44. GRE 隧道配置

§ 【GRE隧道名称】：用于标识一条GRE隧道，以方便进行管理。

% 注意：
修改VPN隧道配置时，隧道名称不可以修改。

1. 添加规则

在上图界面点击“增加”进入GRE隧道参数配置界面，如下图：

GRE隧道配置

启用	☒
对端外网IP	*
对端内网IP	*
对端内网掩码	*
本端隧道IP	*
本端隧道掩码	*
返回GRE列表	

取消

保存

图4-45. GRE 连接配置



- § 【启用状态】：GRE隧道使能开关，缺省为禁用状态。勾选则为启用GRE隧道。
- § 【对端外网IP】：设置GRE隧道对端网络的对外接口IP，常为公网IP（Internet）地址。也可为企业不同内网IP。
- § 【对端内网IP】：设置GRE隧道对端网络的对内接口IP，常为局域网网关，也可以为单个IP地址。
- § 【对端内网掩码】：设置GRE隧道对端内网网络的子网掩码，如果是单台主机则需填写32位掩码。
- § 【本端隧道IP】：设置隧道本端GRE隧道的IP地址。
- § 【本端隧道掩码】：设置隧道本端GRE隧道的网络掩码，最好与通信对端的隧道在一个网段上。

2. 修改GRE隧道配置

要修改某条GRE隧道配置时，在“VPN” à “GRE”便可以进入GRE 隧道配置编辑界面，如下图：

GRE隧道配置

GRE隧道名称	启用	对端外网IP	对端内网IP	对端内网掩码	
neta	启用	222.178.56.3	192.168.20.1	255.255.255.255	 

输入隧道名称,添加隧道:

 增加

图4-46. GRE 配置编辑

当要修改某条已配置好的隧道，在上图中在对应规则行点击 “” 就可以修改。修改的配置界面同图4-46。

3. 删除规则

当不需要某条GRE隧道时，通过图4-46中隧道一栏点击 “” 即可删除相应的GRE隧道。

4.6.4 证书上传管理

路由器涉及的证书介绍

证书是一种安全的认证模式，它通过验证对端的证书是否有效来达到保证数据安全的目的。因此，使用证书认证时，我们需要获取到有效的证书。

目前，该路由器支持 ①证书申请 和 ②其它证书的直接导入。

（1）证书申请：通过填写相应的配置项来获取到证书申请文件，并用该申请文件交给CA签发认证。签发认证的目的是让证书有效。



详细描述: 用户用该路由器证书的申请方式申请一个证书请求文件（后缀名为csr，申请方式详见证书申请），当路由器生成了证书请求文件以后，会跳转到证书上传管理界面。用户可通过下载来获取证书请求文件（路由器生成证书请求文件的同时，也会产生一个私钥，该私钥由路由器自动保存到路由器内部），然后用该证书申请文件到ca认证机构去签发认证。如果通过了ca认证机构，会获得一个由ca签发的证书文件（后缀名为crt），然后用这个签发的证书在路由器的“证书申请文件列表”上传（注意上传的位置，和私钥相对应）。上传成功以后，用户便可以在IPSec配置界面使用该证书（注：还要上传该ca的中心证书，可能还会上传CA的上级CA证书）。

(2) 其它证书导入: IPSec另一端会发给一个有效的证书和私钥，以及CA证书。用户拿到这些证书以后，可以在“上传证书”上传相关的证书（详见下图）。

1) 证书上传管理

当要进行证书上传时，进入“VPN” à “证书管理” à “证书上传管理” 便可以进入IPSec证书上传配置界面，如下图：

证书上传管理

选择上传模式

☒

上传设备证书和私钥

☐

上传CA证书

☐

上传证书吊销文件

浏览...

证书文件

浏览...

私钥文件

上传

证书文件列表

证书标识名	证书类型	私钥文件名	吊销列表文件名	删除
-------	------	-------	---------	----

证书申请文件列表（点击右键-“目标另存为”，可以下载证书请求文件）

证书类型	私钥文件名	证书请求标识名	证书请求文件	上传证书	删除
设备证书	maipu-1800-20.key	maipu-1800-20	maipu-1800-20.csr	浏览... 上传	✖

图4-47. 上传证书



§ 【上传证书】：用于上传在其他设备上申请的证书。此处必须要上传设备证书和私钥，中心证书（ca证书）。上传后的证书将在证书列表中显示出来。证书吊销文件可用于让某个指定证书失去它的有效性。

§ 【证书文件列表】：用于显示上传到路由器的当前的数字证书。

§ 【证书申请文件列表】：用于上传证书文件。此证书文件是在“证书申请”中产生的csr文件由ca签发后得到的证书（crt）（具体申请步骤详见证书申请）。

点击 “ ” 可用删除相关证书。

2) 证书申请

当要进行证书申请时，进入“VPN” à “证书管理” à “证书申请” 便可用进入IPSec证书申请配置界面，如下图：

证书申请

请求文件名	apply	*
密钥长度	512	
国家代码(C)	CN	
省份(ST)	sichuan	
城市街道名(L)	jiuxing	
组织(O)	maipu	
组织单位(OU)	maipu	
通用名(CN)	commonname	*
邮箱(emailAddress)	username@maipu	

复位

提交

图4-48. 证书申请

§ 【请求文件名】：（必填项）用于证书请求保存文件名和保存私钥文件名，确保其唯一性。（最终获得*.csr，*为请求文件名）。

§ 【密钥长度】：（必填项）私钥的密钥长度。

§ 【国家代码】：（可选项）一般选择CN。

§ 【省份】：（可选项）一般填写自己所在的省份。

§ 【城市街道名】：（可选项）一般填写自己所在的街道名。

§ 【组织】：（可选项）一般填写自己所在组织的名称。

§ 【组织单位】：（可选项）一般填写自己所在单位。



- § 【通用名】：（必填项）注意不能填写特殊字符，如：* & ^。（通用名唯一）
- § 【邮箱】：（可选项）自己或公司的e-mail地址。

点击“提交”按钮，页面跳转到证书上传管理界面，在证书申请文件列表中可以下载、删除证书请求文件。

& 提示:

- 1. 当在证书申请文件列表中下载证书请求文件时，推荐使用鼠标移放到对应证书请求文件上，点击右键à“目标另存为”方式下载。
- 2. 如果使用迅雷等第三方下载工具，需要勾选“只从原始地址下载”选项。

4.7 状态

通过“状态”菜单，用户可以查看MP1800-20路由器当前的配置及运行状态等信息，具体包括：

- n 系统日志
- n 系统信息
- n IPSec隧道状态
- n 拨号接口状态
- n LAN状态
- n 路由信息
- n DHCP信息
- n 连接信息

4.7.1 系统日志

“系统日志”主要显示MP1800-20路由器日志信息。

进入“状态”à“系统日志”，看到如下界面：

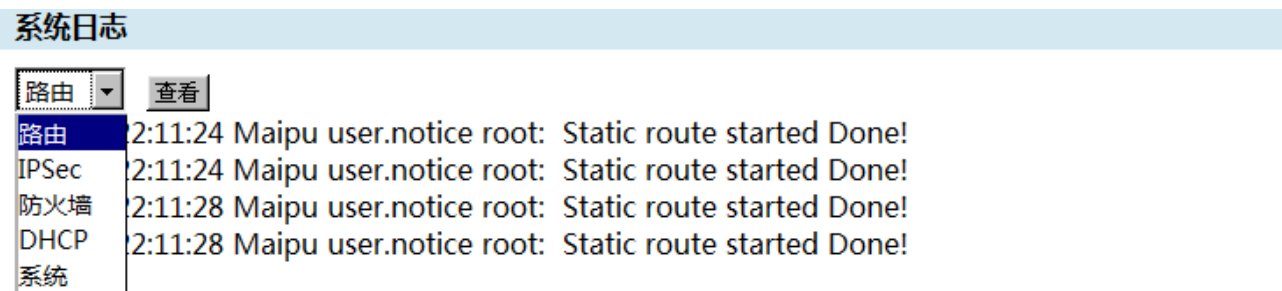


图4-49. 系统日志



& 提示：

系统日志分为路由、IPSEC、防火墙、DHCP、系统5种，用户可分别在下拉菜单中选取查看。

4.7.2 系统信息

系统信息主要显示MP1800-20路由器的硬件、软件版本信息，便于您以后更新系统时，可根据版本信息选择相应的升级文件进行升级。

进入“状态” à “系统信息”，看到如下界面：

系统信息	
基本信息	
设备型号	RM1800-20C
设备序列号	c00008
硬件版本	001
软件版本	1.0.9
编译时间	2011-05-23 22:12
设备主频	320MHz
设备内存	32M
设备信息	
Modem信息	模块已连接
SIM卡信息	中国电信

图4-50. 系统信息

- § 【设备型号】：MP1800-20产品型号信息，如RM1800-20C。
- § 【设备序列号】：设备出厂序列号信息。
- § 【硬件版本】：当前硬件版本信息。
- § 【软件版本】：当前操作系统、应用软件版本信息。
- § 【设备主频】：MP1800-20设备主频信息。
- § 【设备内存】：MP1800-20设备内存信息。
- § 【SM1（国密）卡信息】：当前SM1（国密）卡连接信息。如果设备不支持该模块，则不会显示。
- § 【Modem信息】：当前Modem连接信息。
- § 【SIM信息】：当前SIM连接信息。



4.7.3 IPSec隧道状态

隧道状态显示IPSec隧道信息，显示隧道SA信息。

进入“状态” à “隧道状态”，看到如下界面：

IPSec隧道状态

刷新

隧道SA信息

隧道 #1: (192.168.10.0/24[any])182.144.176.250 <-> 119.6.69.212 (100.100.100.0/24[any])
封装: esp, des-cbc, hmac-md5, Tunnel, SPI: 0xccbf027b/0x0c2a7ddb
接收流量: 1020(bytes)/13(packets)
发送流量: 1696(bytes)/13(packets)
生命周期: 28800(s)
运行时间: 0 天 0 小时 8 分 27 秒

当前隧道总数: 1

图4-51. 隧道状态

- § **【SA】**：IPSec安全关联。
- § **【隧道】**：显示隧道两端的网关地址。
- § **【封装】**：显示隧道的安全协议，如esp, ah等；加密算法-认证算法-协商模式（Transport或Tunnel）；两个方向的安全关联的spi（安全参数索引）值。
- § **【接收流量】**：通过隧道，接收到对端发来的数据流量。
- § **【发送流量】**：通过隧道，发送到对端的数据流量。
- § **【生命周期】**：IPSec SA的最大使用时间。
- § **【运行时间】**：隧道建立的时间长度。
- § **【当前隧道总数】**：设备中已经建立的隧道总数。

4.7.4 拨号接口状态

拨号接口状态页面显示了拨号接口状态、拨号接口流量信息、移动网络设备信息。

拨号接口状态显示了MP1800-20路由器所使用的无线网络模块连接信息、网络连接信息、以及SIM卡是否在位等信息。通过这些信息您可以快速的了解当前设备无线网络连接状况。如下图：



拨号接口状态

重新拨号 刷新

拨号接口状态	模块已连接, SIM卡在位, 网络已连接
网络提供商	中国电信
网络模式	CDMA/HDR HYBRID
信号强度	▬▬▬ (-89 dBm)
IP 地址	182.144.137.167
网关	172.22.212.123

图4-52. 拨号接口状态

拨号接口流量信息显示了当前设备无线网络接口流量信息。如下图：

拨号接口流量信息	
收到包数	14
收到错误包数	2
收到被丢弃包数	0
收到字节数	606
发送包数	184
发送错误包数	0
发送被丢弃包数	0
发送字节数	13245

图4-53. 拨号接口流量信息

移动网络设备信息示了当前设备已连接的无线网络设备信息。如下如图所示：

移动网络设备信息	
设备厂商	Huawei
设备型号	EM660

图4-54. 移动网络设备信息



4.7.5 LAN状态

LAN状态显示了当前局域网设置、连接状态以及LAN 接口进行数据接收和转发的流量情况，进入“状态” à “LAN状态”，看到如下界面：

LAN状态	
IP 地址	192.168.10.1
子网掩码	255.255.255.0
物理地址	00:01:7A:C0:00:08

图4-53. LAN状态

- § 【IP地址】：显示LAN口已配置的IP地址。
- § 【子网掩码】：显示所配置的LAN接口所在的网络地址号。
- § 【物理地址】：显示LAN网口卡物理地址，此地址一般情况下固定和是唯一的。

LAN流量信息	
收到包数	8664
收到错误包数	0
收到被丢弃包数	0
收到字节数	965064
发送包数	8735
发送错误包数	0
发送被丢弃包数	0
发送字节数	6129277

图4-54. LAN流量信息

- § 【收到包数】：显示LAN 口从上线来已接收的数据报数量总和。
- § 【收到错误包数】：显示LAN 口从上线来已接收的错误数据报数量。
- § 【收到被丢弃包数】：显示LAN 口从上线来已接收的被丢弃的数据报数量。
- § 【收到字节数】：显示LAN 口从上线来已接收的数据字节数量。
- § 【发送包数】：显示LAN 口从上线来已发送的数据报数量总和。
- § 【发送错误包数】：显示LAN 口从上线来已发送的错误数据报数量。
- § 【发送被丢弃包数】：显示LAN 口从上线来已发送被丢弃数据报数量。
- § 【发送字节数】：显示LAN 口从上线来已发送的数据字节数量。



4.7.6 路由信息

查看MP1800-20路由器所有路由信息，请进入“状态” à “路由信息” 查看系统当前所有路由信息。如下图：

路由信息					刷新
局域网	目的地址	子网掩码	网关	距离	
lan	192.168.10.0	255.255.255.0	0.0.0.0	0	

图4-55. 路由信息

4.7.7 DHCP信息

DHCP客户端信息列表显示了当前MP1800-20路由器所有DHCP客户端的IP分配信息。进入“状态” à “DHCP信息” 可以查看到自动分配的地址情况，如下图：

DHCP信息			
主机名	IP	MAC	剩余时间
maipu-cc951180a	192.168.10.100	00:1f:c6:59:c2:0f	10h 52m 18s

图4-56. DHCP信息

4.7.8 连接信息

连接信息显示了当前MP1800-20路由器所有的ARP表的信息和当前系统的连接信息。进入“状态” à “连接信息” 可以查看到系统连接的状态，如下图：



连接信息

刷新

ARP表

IP	MAC	接口
192.168.10.240	00:1F:C6:59:C2:0F	br-lan

连接信息

局域网	协议	源IP	目的IP
IPv4	TCP	192.168.10.240	192.168.10.1
IPv4	TCP	192.168.10.240	192.168.10.1

图4-57. 连接信息



第5章 常见问题解答

本章主要向您提供了一些MP1800-20路由器在使用过程中的常见问题，并提供了处理的措施或方法。同时也希望在您的大力支持下常见问题解答更加全面和充实。

【问题1】：为什么我的计算机连接MP1800-20路由器LAN口后,相应的LAN口指示灯不亮？

答：首先请确认连接接口都已插紧,接着确认已排除网线问题,其次请检查计算机网卡,PCI插槽等问题.如还不能解决,请再次检查相关设备。

【问题2】：为什么无法登录MP1800-20路由器管理界面？

答：您可以尝试从以下几个方面确认问题：

1. 请确认您的计算机IP地址与路由器LAN在同一个网段(具体请参考3.3节内容说明)
2. 请检查网线是否连接到了MP1800-20 路由器正确的接口(LAN),计算机网卡指示灯、MP1800-20路由器对应LAN口指示灯是否都常亮
3. 请确保您计算机IE浏览器设置正确,正确设置如下：
4. 打开IE,找到“工具”à“Internet选项”à“连接”，删除所有“拨号和虚拟连接”，或将各条目设置为“从不进行拨号连接”如下图所示。在“文件”或工具菜单并取消IE浏览器的脱机状态（点击去掉“✓”号）。





【问题3】：使用MP1800-20路由器可以上网，但是网上邻居不能互访，为什么？

答：网上邻居访问无需对MP1800-20路由器做任何配置，如果局域网需要网上邻居访问，请确认所要访问的计算机系统设置。

【问题4】：MP1800-20路由器总是提示软件升级失败，怎么办？

答：请查看对应的软件版本是否符合产品型号升级。如果文件确定OK，请确保供电环境的稳定性。

【问题6】：如何将MP1800-20路由器恢复出厂设置？

答：请在MP1800-20路由器前面板上找到标识为“RESET”的圆孔，通过小的尖状物按压RESET按键5~10秒，同时观察前面板SYS灯由闪烁状态变为常亮，数秒钟后，如果指示灯闪烁，说明已经恢复成功。

【问题7】：不小心忘记了MP1800-20路由器密码，怎么办？

答：您需要使用RESET按键将系统配置恢复到出厂状态（密码：admin）。

【问题7】：希望获取更多的操作和应用支持，怎么办？

答：请您拨打迈普公司技术专线：**400-886-8669**。